

AS

(19)



JAPANESE PATENT OFFICE

## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000165376 A**

(43) Date of publication of application: 16.06.00

(51) Int. Cl.

**H04L 9/14****G11B 20/10****H04L 9/32****H04L 12/28**

(21) Application number: 10333218

(22) Date of filing: 24.11.98

(71) Applicant:

**MATSUSHITA ELECTRIC IND CO LTD**

(72) Inventor:

**YAMADA MASAZUMI  
IZUKA HIROYUKI  
NISHIMURA TAKUYA  
TAKECHI HIDEAKI  
KUNO YOSHIKI  
HAMAMOTO YASUO**

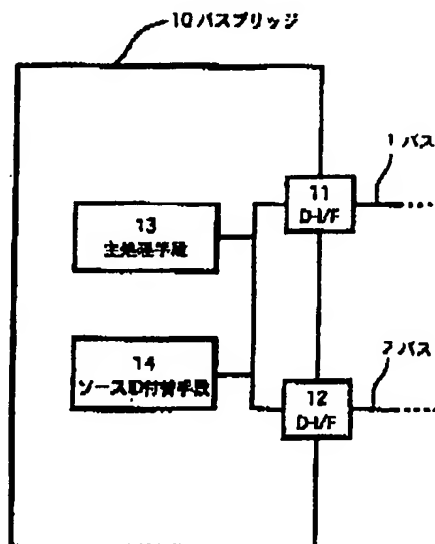
## (54) BUS BRIDGE AND RECORDING MEDIUM

(57) Abstract:

**PROBLEM TO BE SOLVED:** To provide a bus bridge by which a device at a destination can discriminate a sender device directly or indirectly in the case of conducting data transfer using a data packet like an isochronous packet among different buses in compliance with the AV protocol where the sender device can be specified only in a single bus.

**SOLUTION:** The bus bridge 10 consists of D-I/F 11, 12 that transfer data directly to buses 1, 2, a main processing means 13 that applies processing such as clock adjustment processing similar to that for a conventional bus bridge to a packet sent from each bus and a source ID replacement means 14. The source ID replacement means 14 uses a source ID in an isochronous packet for a node ID to specify the bus bridge 10 in a destination bus or replaces a node to specify the sender device in a sender bus with a node ID to specify the bus bridge in a destination bus.

COPYRIGHT: (C)2000,JPO



BEST AVAILABLE COPY

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開2000-165376

(P2000-165376A)

(43)公開日 平成12年6月16日(2000.6.16)

(51)IntCl <sup>1</sup>	識別記号	FI	チーコード*(参考)	
H04L 9/14		H04L 9/00	641	5D044
G11B 20/10		G11B 20/10	D	5J104
H04L 9/32		H04L 9/00	675A	5K033
12/28		11/00	310Z	

審査請求 未請求 請求項の数15 OL (全 17 頁)

(21)出願番号 特願平10-333216

(22)出願日 平成10年11月24日(1998.11.24)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 山田 正純

大阪府門真市大字門真1006番地 松下電器

産業株式会社内

(72)発明者 飯塚 裕之

大阪府門真市大字門真1006番地 松下電器

産業株式会社内

(74)代理人 100092794

弁理士 松田 正道

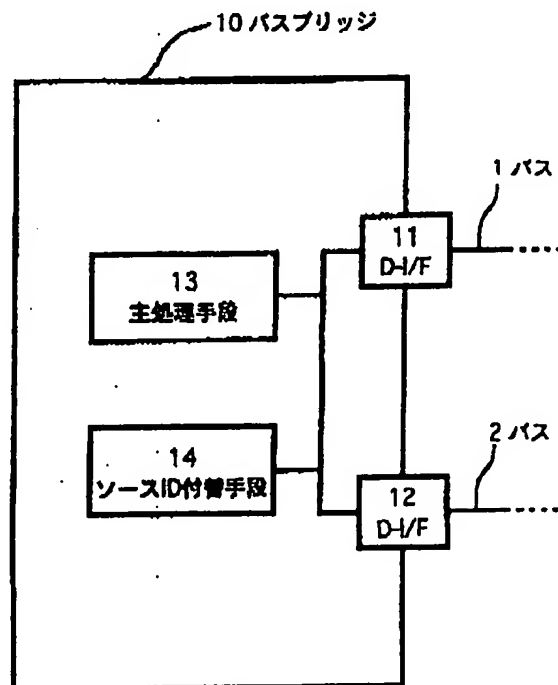
最終頁に続く

(54)【発明の名称】 バスブリッジおよび記録媒体

(57)【要約】

【課題】 AVプロトコルに準拠したアイソクロノスケットのような単一バス内でのみ送信元の機器を特定できるようなデータケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が直接または間接的に送信元の機器を判別できるバスブリッジを提供する。

【解決手段】 バスブリッジ10は、バス1、2と直接データの転送を行うD-1/F11、12と、各バスから送信されてきたケットに対してクロック調整処理等の従来のバスブリッジと同様の処理を行う主処理手段13と、ソースID付替手段14とで構成されており、ソースID付替手段14は、アイソクロノスケットのソースIDを、受信先バス内でバスブリッジ10を特定するノードIDとする、または、送信元バス内で送信元機器を特定するノードIDから、受信先バス内でバスブリッジ10を特定するノードIDに付け替える。



(2)

特開2000-165376

## 【特許請求の範囲】

【請求項1】 それぞれに一つまたは複数の機器が接続された複数のバス間を接続し、異なる前記バスにそれぞれ接続されている前記機器間のデータ転送を仲介するバスブリッジにおいて、

前記データ転送を仲介されるストリームの送信元機器が接続されている前記バスを送信元バスとし、前記ストリームの受信先機器が接続されている前記バスを受信先バスとすると、

前記ストリームのデータ用パケットの送信元の識別子であるソースIDを、前記受信先バス内で前記バスブリッジ自身を特定するノードIDとする、または、前記送信元バス内で前記送信元機器を特定するノードIDから、前記受信先バス内で前記バスブリッジ自身を特定するノードIDに付け替えるID付け手段を備えることを特徴とするバスブリッジ。

【請求項2】 前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、

前記受信先機器からの前記ストリームに対応する認証要求および認証の手續きに関するパケットを前記送信元機器へ送信する認証要求送受信手段と、

前記送信元機器から前記ストリームに対応する前記暗号化鍵および認証の手續きに関するパケットを受信して前記受信先機器へ送信する暗号化鍵送受信手段と、

前記送信元機器から、前記ストリームに対応し、前記暗号化鍵によって暗号化された前記データを受信して前記受信先機器へ送信するデータ送受信手段と、

前記認証要求および認証の手續きに関するパケットを前記送信元機器へ送信する際、前記認証要求および認証の手續きに関するパケットの受信先の識別子であるディスティネーションIDを、前記受信先バスを特定するバスIDと前記受信先バス内で前記バスブリッジ自身を特定するノードIDとの組合せから、前記送信元バスを特定するバスIDと前記送信元バス内で前記送信元機器を特定するノードIDとの組合せに付け替え、前記認証要求および認証の手續きに関するパケットの送信元の識別子であるソースIDを、前記受信先バスを特定するバスIDと前記受信先バス内で前記受信先機器を特定するノードIDとの組合せから、前記送信元バスを特定するバスIDと前記送信元バス内で前記バスブリッジ自身を特定するノードIDとの組合せに付け替え、前記暗号化鍵および認証の手續きに関するパケットを前記受信先機器へ送信する際、前記暗号化鍵および認証の手續きに関するパケットの受信先の識別子であるディスティネーションIDを、前記送信元バスを特定するバスIDと前記送信元バス内で前記バスブリッジ自身を特定するノードIDとの組合せから、前記受信先バスを特定するバスIDと前記受信先バス内で前記受信先機器を特定するノードIDとの組合せに付け替え、前記暗号化鍵および認証の手續きに関するパケットの送信元の識別子であるソースID

IDを、前記送信元バスを特定するバスIDと前記送信元バス内で前記送信元機器を特定するノードIDとの組合せから、前記受信先バスを特定するバスIDと前記受信先バス内で前記バスブリッジ自身を特定するノードIDとの組合せに付け替える第2のID付け手段とを備えることを特徴とする請求項1に記載のバスブリッジ。

【請求項3】 前記受信先バス内で前記バスブリッジ自身を特定する前記ノードID1つに対して、前記受信先バスに前記受信先バス以外の前記バスから転送される前記ストリーム数を、使用許諾情報のうちデータ暗号化を要する種類毎に1つ以下に制限することを特徴とする請求項2に記載のバスブリッジ。

【請求項4】 前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、

前記受信先機器からの前記ストリームに対応する認証要求および認証の手續きに関するパケットを前記送信元機器へ送信する認証要求送受信手段と、

前記送信元機器から前記ストリームに対応する前記暗号化鍵および認証の手續きに関するパケットを受信して前記受信先機器へ送信する暗号化鍵送受信手段と、

前記送信元機器から、前記ストリームに対応し、前記暗号化鍵によって暗号化された前記データを受信して前記受信先機器へ送信するデータ送受信手段と、

前記送信元バスおよび前記送信元機器を特定できる送信元識別子を、前記データ用パケットの所定の位置に書き込む識別子書き込み手段とを備え、

前記受信先機器は、前記データ用パケットから前記送信元識別子を読み取り、前記認証要求および認証の手續きに関するパケットの所定の位置に、前記受信先バスおよび前記受信先機器自身を特定できる受信先識別子および前記送信元識別子を書き込んで送信し、

前記認証要求送受信手段は、前記認証要求および認証の手續きに関するパケットを受信して、前記送信元識別子を読み取り、これに基づいて、前記認証要求および認証の手續きに関するパケットを前記送信元機器へ送信し、前記送信元機器は、前記認証要求および認証の手續きに関するパケットを受信して、前記送信元識別子を読み取り、前記暗号化鍵および認証の手續きに関するパケットの所定の位置に、前記送信元識別子および前記受信先識別子を書き込んで送信し、

前記暗号化鍵送受信手段は、前記暗号化鍵および認証の手續きに関するパケットを受信して、前記受信先識別子を読み取り、これに基づいて、前記暗号化鍵および認証の手續きに関するパケットを前記受信先機器へ送信することを特徴とする請求項1に記載のバスブリッジ。

【請求項5】 前記受信先機器は、前記認証要求および認証の手續きに関するパケットの前記ソースIDおよび前記ディスティネーションIDの位置に、それぞれ前記受信先識別子および前記送信元識別子を書き込んで送信し、

3

前記送信元機器は、前記暗号化鍵および認証の手續きに関するパケットの前記ソースIDおよび前記ディステーションIDの位置に、それぞれ前記送信元識別子および前記受信先識別子を書き込んで送信することを特徴とする請求項4に記載のバスブリッジ。

【請求項6】 前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、

前記送信元機器および前記受信先機器とそれぞれ前記ストリームに対応する認証を行う認証手段と、

前記送信元機器から受け渡された、前記ストリームに対応する前記暗号化鍵を保持し、これを、前記受信先機器からの要求に応じて、前記受信先機器へ送信する暗号化鍵保持手段とを備えることを特徴とする請求項1に記載のバスブリッジ。

【請求項7】 前記受信先バス内で前記バスブリッジ自身を特定する前記ノードID1つに対して、前記受信先バスに前記受信先バス以外の前記バスから転送される前記ストリーム数を、使用許諾情報のうちデータ暗号化を要する種類毎に1つ以下に制限することを特徴とする請求項6に記載のバスブリッジ。

【請求項8】 前記暗号化鍵は、定期的または定期的に更新生成されるデータ暗号化鍵と、前記データ暗号化鍵の暗号化に用いる鍵交換用鍵とで構成され、前記データ暗号化鍵は、送信時においては、前記鍵交換用鍵により暗号化されていることを特徴とする請求項2～7のいずれかに記載のバスブリッジ。

【請求項9】 前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、

前記送信元機器および前記受信先機器とそれぞれ前記ストリームに対応する認証を行う認証手段と、

前記データを前記暗号化鍵によって解読する暗号解読手段と、

前記解読されたデータをブリッジ用鍵によって再暗号化する再暗号化手段と、

前記送信元機器から、前記ストリームに対応する前記暗号化鍵、および、前記暗号化鍵によって暗号化された前記ストリームに対応する前記データを受信する受信手段と、

前記ブリッジ用鍵と前記再暗号化されたデータとを前記受信先機器へ送信する送信手段とを備えることを特徴とする請求項1に記載のバスブリッジ。

【請求項10】 前記ブリッジ用鍵は、1つの前記ストリームに対応する前記暗号化鍵と同じものであり、

前記ブリッジ用鍵と同じ前記暗号化鍵により暗号化された前記データは、前記暗号解読手段による解読および前記再暗号化手段による再暗号化を行われずに、前記受信先機器へ送信されることを特徴とする請求項9に記載のバスブリッジ。

【請求項11】 前記暗号化鍵は、定期的または定期的に更新生成されるデータ暗号化鍵と、前記データ暗号

(3)

特開2000-165376

4

化鍵の暗号化に用いる鍵交換用鍵とで構成され、

前記データ暗号化鍵は、送信時においては、前記鍵交換用鍵により暗号化されており、

前記ブリッジ用鍵は、定期的または定期的に更新生成されるブリッジ用暗号化鍵と、前記ブリッジ用暗号化鍵の暗号化に用いるブリッジ用鍵交換用鍵とで構成され、前記受信手段は、前記送信元機器から、前記データ暗号化鍵によって暗号化された前記データ、前記鍵交換用鍵によって暗号化された前記データ暗号化鍵および前記鍵交換用鍵を受信し、

前記暗号解読手段は、前記データ暗号化鍵を前記鍵交換用鍵によって解読し、前記データを前記解読されたデータ暗号化鍵によって解読し、

前記再暗号化手段は、前記解読されたデータを前記ブリッジ用暗号化鍵によって再暗号化し、前記ブリッジ用暗号化鍵を前記ブリッジ用鍵交換用鍵によって再暗号化し、

前記送信手段は、前記ブリッジ用鍵交換用鍵、前記ブリッジ用鍵交換用鍵によって再暗号化された前記ブリッジ用暗号化鍵と、前記ブリッジ用暗号化鍵によって再暗号化された前記データとを前記受信先機器へ送信することを特徴とする請求項9に記載のバスブリッジ。

【請求項12】 前記ブリッジ用暗号化鍵および前記ブリッジ用鍵交換用鍵は、1つの前記ストリームに対応する前記データ暗号化鍵および前記鍵交換用鍵とそれぞれ同じものであり、

前記1つのストリームに対応する前記データ、前記データ暗号化鍵および前記鍵交換用鍵の転送を行う場合、

前記ブリッジ用暗号化鍵と同じ前記データ暗号化鍵により暗号化された前記データおよび前記ブリッジ用鍵交換用鍵と同じ前記鍵交換用鍵により暗号化された前記データ暗号化鍵は、前記暗号解読手段による解読および前記再暗号化手段による再暗号化を行われずに、前記受信先機器へ送信されることを特徴とする請求項11に記載のバスブリッジ。

【請求項13】 前記ブリッジ用暗号化鍵は、1つの前記ストリームに対応する前記データ暗号化鍵と同じものであり、

前記1つのストリームに対応する前記データ、前記データ暗号化鍵および前記鍵交換用鍵の転送を行う場合、

前記受信手段は、前記送信元機器から、前記データ暗号化鍵によって暗号化された前記データ、前記鍵交換用鍵によって暗号化された前記データ暗号化鍵および前記鍵交換用鍵を受信し、

前記暗号解読手段は、前記データ暗号化鍵を前記鍵交換用鍵によって解読し、

前記再暗号化手段は、前記データ暗号化鍵を前記ブリッジ用暗号化鍵とし、これを前記ブリッジ用鍵交換用鍵によって再暗号化し、

前記送信手段は、前記ブリッジ用鍵交換用鍵、前記ブリ

(4)

特開2000-165376

5

6

ッジ用鍵交換用鍵によって再暗号化された前記ブリッジ用暗号化鍵と、前記暗号解読手段による解読および前記再暗号化手段による再暗号化が行われなかった前記データとを前記受信先機器へ送信することを特徴とする請求項11に記載のバスブリッジ。

【請求項14】 前記ブリッジ用鍵交換用鍵は、1つの前記ストリームに対応する前記鍵交換用鍵と同じものであり、

前記1つのストリームに対応する前記データ、前記データ暗号化鍵および前記鍵交換用鍵の転送を行う場合、

前記受信手段は、前記送信元機器から、前記データ暗号化鍵によって暗号化された前記データ、前記鍵交換用鍵によって暗号化された前記データ暗号化鍵および前記鍵交換用鍵を受信し、

前記暗号解読手段は、前記データ暗号化鍵を前記鍵交換用鍵によって解読し、前記データを前記解読されたデータ暗号化鍵によって解読し、

前記再暗号化手段は、前記解読されたデータを前記ブリッジ用暗号化鍵によって再暗号化し、前記鍵交換用鍵を前記ブリッジ用鍵交換用鍵とし、これによって前記ブリッジ用暗号化鍵を再暗号化し、

前記送信手段は、前記ブリッジ用鍵交換用鍵、前記ブリッジ用鍵交換用鍵によって再暗号化された前記ブリッジ用暗号化鍵と、前記ブリッジ用暗号化鍵によって再暗号化された前記データとを前記受信先機器へ送信することを特徴とする請求項11に記載のバスブリッジ。

【請求項15】 請求項1～14のいずれかに記載の、各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納することを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、それぞれに一つまたは複数の機器が接続された複数のバス間を接続し、異なる前記バスにそれぞれ接続されている前記機器間のデータ転送を仲介するバスブリッジ、および、前記バスブリッジの各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納する記録媒体に関するものである。

【0002】

【従来の技術】大量のデータ転送を高速かつ高品質に行えるデジタル・インターフェースとし、IEEE1394規格(IEEE:THE INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, INC)を用いた高速シリアル・バス・インターフェース(以下、「IEEE1394バス」と記す。)が近年注目されてきている。

【0003】IEEE1394規格におけるデータ転送には、映像信号や音声信号等の同期データの転送に適したアイソクロノス通信と、制御信号等の非同期データの転送に適したエイシンクロノス通信とがあり、両通信はIEEE1394バス上で混在することが可能である。

【0004】アイソクロノス通信は、いわゆる放送型の通信であり、IEEE1394バス上のある装置が出力するアイソクロノスパケットは、同バス上の全ての装置が受信することができる。

【0005】これに対してエイシンクロノス通信は、1対1の通信と放送型通信の両方がある。そして、バス上のある装置が出力するエイシンクロノスパケットには、パケットヘッダー内に、そのパケットを受信すべき装置をあらわす識別子であるディスティネーションIDが含まれており、そのディスティネーションIDが特定の装置をあらわす時にはその識別子で指定された装置が当該エイシンクロノスパケットを受信し、ディスティネーションIDがブロードキャストをあらわす時には同バス上の全ての装置が当該エイシンクロノスパケットを受信する。なお、エイシンクロノスパケットには、パケットヘッダー内に、そのパケットを送信している送信装置をあらわす識別子であるソースIDも含まれている。このディスティネーションIDおよびソースIDには、それぞれ16ビットが割り当てられており、そのうちの10ビットには機器が接続されているバスを特定するバスIDが書き込まれ、6ビットにはバス内で当該機器を特定するノードIDが書き込まれる。

【0006】また、IEEE1394規格を用いてデジタル音声信号やデジタル映像信号等を転送したり、IEEE1394バス上につながれた機器間でデータ伝送経路の接続管理を行うための規格として、IEC(IEC: International Electrotechnical Commission 国際電気標準会議)においてIEC61883規格(以下、「AVプロトコル」と記す。)が検討されている。AVプロトコルにおいては、映像音声データはアイソクロノスパケット内に配置されて転送される。また、アイソクロノスパケットはCIPヘッダ(CIP: Common Isochronous Packet)を含む。CIPヘッダ内には映像音声データの種別を示す識別情報や、アイソクロノスパケットを送信している送信装置の装置をあらわす識別子であるソースID等の情報が含まれている。

【0007】図5は、AVプロトコルに準拠したアイソクロノスパケットのフォーマットを示す図である。アイソクロノスパケットは、アイソクロノスパケットヘッダ900、ヘッダCRC901、アイソクロノスペイロード902、データCRC903からなる。

【0008】アイソクロノスパケットヘッダ900にはタグ907が含まれる。タグ907は、その値が1である時には、そのアイソクロノスパケットがAVプロトコルに準拠したアイソクロノスパケットであることを示す。タグ907の値が1であるとき、即ち、そのアイソクロノスパケットがAVプロトコル準拠のアイソクロノスパケットである時には、アイソクロノスペイロード902の先頭にCIPヘッダ904が含まれる。

【0009】また、アイソクロノスパケットヘッダ90

(5)

特開2000-165376

7

8

0中のChannelフィールド911には、バス内での転送に用いられているチャンネル番号が書き込まれる。

【0010】また、アイソクロノスケットヘッダ900には、Syフィールド910が含まれる。AVプロトコル選択のアイソクロノスケットである時には、Syフィールドはデータ保護情報(使用許諾情報)等を格納するために使用される。具体的にはEMI(Encryption Mode Indicator)と呼ばれる使用許諾情報の代表値およびデータ暗号化モードを示す2ビットの情報と、データ暗号化鍵の更新タイミングを示すOdd/Evenフラグと呼ばれる1ビットの情報を含む。Syフィールド910に格納されたEMI値が「00」である時には、送信対象となるデータ(後述する実データ905)が、コピーが自由に行えるデータである事を示している。また、「10」である時には、そのデータが、1回のみコピー可能であることを、更に、「11」である時には、そのデータが、コピー禁止であることを示している。

【0011】CIPヘッダ904の中には、当該アイソクロノスケットを出力している送信元の装置の識別子であるソースID906が含まれる。このソースID906は、6ビットの長さを有しており、一つのバス内で当該送信元の機器を特定するノードIDが書き込まれる。

【0012】また、CIPヘッダ904には、アイソクロノスペイロード902に含まれる実データ905がどのような種類のデータであるかをあらわすFMT908やFDF909が含まれる。

【0013】映像や音声の送信対象となるデータは実データ905に含まれるが、この実データ905は、上述したEMI値が、「10」または「11」である場合には、暗号化されたデータであるが、コピーフリーを意味する「00」の場合には、暗号化はされていない。また、実際の使用許諾情報は、実データ905中に含まれており、一般に、CDの場合はSCMSと、また、DVの場合はCGMS等と呼ばれている。

【0014】以上のようなIEEE1394バスを複数個接続して、異なるIEEE1394バスにそれぞれ接続されている機器間のデータ転送を仲介するバスブリッジが提案されている。図6は、バスブリッジによってデータ転送の仲介が行われる2つのIEEE1394バスを示す概略構成図である。バス1には複数の機器101、102、103、・・・が接続されており、バス2には複数の機器201、202、203、・・・が接続されている。バスブリッジ100は、バス1、2に接続されており、それぞれのバスに接続されている前記機器間のデータ転送を仲介するものである。

【0015】図6のバスブリッジ100のようにIEEE1394バスが接続されたバスブリッジの機能として

は、異なるバスブリッジに接続された機器間のデータ転送において、バス間のクロックの調整を行うこと、送信元のバス側のアイソクロノス・リソースのコピー(帯域確保)、すなわち、バス1中でアイソクロノス通信用に確保された帯域用のパラメータをバス2側でも同様に確保することを行うこと等が挙げられる。

【0016】

【発明が解決しようとする課題】しかしながら、図6で示したようなバスブリッジにおいて、図5で示したようなAVプロトコルに準拠したアイソクロノスケットによって、データ転送を行う場合、アイソクロノスケット中のソースID906には、バス毎に送信元の機器を特定するノードIDが書き込まれるだけで、異なるバス間にまたがったデータ転送を行う場合においては、当該パケットが、受信側と同一のバスに接続された機器から送信されたパケットなのか、異なるバスに接続された機器から送信されたパケットなのか、判別がつかなくなってしまう。

【0017】すなわち、図6において、アイソクロノスケットがバス1に接続された機器103から出力されたものであるとすると、当該アイソクロノスケット中のソースID906には、バス1内で機器103を特定するための識別子であるノードID「3」が書き込まれている。このアイソクロノスケットがバスブリッジ100を介してバス2側へ転送され、バス2に接続された機器202が受信したとすると、機器202は、当該アイソクロノスケットが、機器103から送信されてきたものなのか、機器203から送信されてきたものなのか、判別がつかなくなってしまう。

【0018】ソースID906にノードIDだけでなく、バスを特定するバスID(10ビット)を書き込めれば、上記問題は解決するが、ノードIDは6ビットで定義されるものであり、アイソクロノスケット中のソースID906は6ビットの割り当てしかないため、バスIDの書き込が行われる余地はない。

【0019】通常のアイソクロノスケットによるデータ転送は、放送型の1方向転送であるため、上述したような送信元の機器を判別する必要はないが、転送されるデータの内容・特性等によっては、送信元の機器を判別する必要が生じる。特に、アイソクロノスケット中のSyフィールド910に格納されたEMI値が「10」または「11」である場合、すなわち、当該アイソクロノスケットのデータが、1回のみコピー可能である、または、コピー禁止である場合には、実データは暗号化が施されて転送されるため、暗号解読用の鍵の受け渡しのための認証等を送信元の機器と行う必要があるため、送信元の機器の判別は不可欠なものとなってくる。また、IEEE1394バスにおいては、同一機器から送信される暗号化データの暗号化鍵は前記EMI値の示す暗号化モード毎、すなわちデータ暗号化を要する種類毎

(6)

特開2000-165376

9

10

に同一のものをを用いることにしているため、受信先バスであるバス2内では、同一のノードID、同一種類のEMIに対して、2つ以上の異なった暗号化鍵が使われているようにみなされてしまい、受信側の機器202では、どの暗号化鍵によってデータ解説を行うのが判別できなくなってしまう。さらに、送信元の機器が暗号化鍵を定期的または不定期的に更新する場合においては、機器毎に更新のタイミングが異なるので、解説に真に必要な鍵を受信側機器が判別することは困難である。

【0020】本発明は、上述した従来のバスブリッジが有する課題を考慮し、AVプロトコルに準拠したアイソクロノスケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が直接または間接的に送信元の機器を判別できるバスブリッジを提供することを目的とするものである。さらに、上記に加えて、実データが暗号化されて送信される場合、前記送信元の機器と前記受信先の機器との間での認証・鍵交換が確実に行われるバスブリッジを提供することを目的とするものである。

【0021】また、前記バスブリッジの各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納する記録媒体を提供することを目的とするものである。

【0022】

【課題を解決するための手段】上述した課題を解決するために、第1の本発明（請求項1に記載の本発明に対応）は、それぞれに一つまたは複数の機器が接続された複数のバス間を接続し、異なる前記バスにそれぞれ接続されている前記機器間のデータ転送を仲介するバスブリッジにおいて、前記データ転送を仲介されるストリームの送信元機器が接続されている前記バスを送信元バスとし、前記ストリームの受信先機器が接続されている前記バスを受信先バスとすると、前記ストリームのデータ用パケットの送信元の識別子であるソースIDを、前記受信先バス内で前記バスブリッジ自身を特定するノードIDとする、または、前記送信元バス内で前記送信元機器を特定するノードIDから、前記受信先バス内で前記バスブリッジ自身を特定するノードIDに付け替えるID付替手段を備えることを特徴とするバスブリッジである。

【0023】また、第2の本発明（請求項2に記載の本発明に対応）は、前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、前記受信先機器からの前記ストリームに対応する認証要求および認証の手續きに関するパケットを前記送信元機器へ送信する認証要求送受信手段と、前記送信元機器から前記ストリームに対応する前記暗号化鍵および認証の手續きに関するパケットを受信して前記受信先機器へ送信する暗号化鍵送受信手段と、前記送信元機器から、前記ストリームに

応し、前記暗号化鍵によって暗号化された前記データを受信して前記受信先機器へ送信するデータ送受信手段と、前記認証要求および認証の手續きに関するパケットを前記送信元機器へ送信する際、前記認証要求および認証の手續きに関するパケットの受信先の識別子であるディスティネーションIDを、前記受信先バスを特定するバスIDと前記受信先バス内で前記バスブリッジ自身を特定するノードIDとの組合せから、前記送信元バスを特定するバスIDと前記送信元バス内で前記送信元機器を特定するノードIDとの組合せに付け替え、前記認証要求および認証の手續きに関するパケットの送信元の識別子であるソースIDを、前記受信先バスを特定するバスIDと前記受信先バス内で前記受信先機器を特定するノードIDとの組合せから、前記送信元バスを特定するバスIDと前記送信元バス内で前記バスブリッジ自身を特定するノードIDとの組合せに付け替え、前記暗号化鍵および認証の手續きに関するパケットを前記受信先機器へ送信する際、前記暗号化鍵および認証の手續きに関するパケットの受信先の識別子であるディスティネーションIDを、前記送信元バスを特定するバスIDと前記送信元バス内で前記バスブリッジ自身を特定するノードIDとの組合せから、前記受信先バスを特定するバスIDと前記受信先バス内で前記受信先機器を特定するノードIDとの組合せに付け替え、前記暗号化鍵および認証の手續きに関するパケットの送信元の識別子であるソースIDを、前記送信元バスを特定するバスIDと前記送信元バス内で前記送信元機器を特定するノードIDとの組合せから、前記受信先バスを特定するバスIDと前記受信先バス内で前記バスブリッジ自身を特定するノードIDとの組合せに付け替える第2のID付替手段とを備えることを特徴とする第1の本発明のバスブリッジである。

【0024】また、第3の本発明（請求項4に記載の本発明に対応）は、前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、前記受信先機器からの前記ストリームに対応する認証要求および認証の手續きに関するパケットを前記送信元機器へ送信する認証要求送受信手段と、前記送信元機器から前記ストリームに対応する前記暗号化鍵および認証の手續きに関するパケットを受信して前記受信先機器へ送信する暗号化鍵送受信手段と、前記送信元機器から、前記ストリームに対応し、前記暗号化鍵によって暗号化された前記データを受信して前記受信先機器へ送信するデータ送受信手段と、前記送信元バスおよび前記送信元機器を特定できる送信元識別子を、前記データ用パケットの所定の位置に書き込む識別子書込手段とを備え、前記受信先機器が、前記データ用パケットから前記送信元識別子を読み取り、前記認証要求および認証の手續きに関するパケットの所定の位置に、前記受信先バスおよび前記受信先機器自身を特定できる受信先識別子および前記送信元識別子



(7)

特開2000-165376

11

を書き込んで送信し、前記認証要求受信手段が、前記認証要求および認証の手續きに関するパケットを受信して、前記送信元識別子を読み取り、これに基づいて、前記認証要求および認証の手續きに関するパケットを前記送信元機器へ送信し、前記送信元機器が、前記認証要求および認証の手續きに関するパケットを受信して、前記送信元識別子を読み取り、前記暗号化鍵および認証の手續きに関するパケットの所定の位置に、前記送信元識別子および前記受信先識別子を書き込んで送信し、前記暗号化鍵受信手段が、前記暗号化鍵および認証の手續きに関するパケットを受信して、前記受信先識別子を読み取り、これに基づいて、前記暗号化鍵および認証の手續きに関するパケットを前記受信先機器へ送信することを特徴とする第1の本発明のバスブリッジである。

【0025】また、第4の本発明（請求項6に記載の本発明に対応）は、前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、前記送信元機器および前記受信先機器とそれぞれ前記ストリームに対応する認証を行う認証手段と、前記送信元機器から受け渡された、前記ストリームに対応する前記暗号化鍵を保持し、これを、前記受信先機器からの要求に応じて、前記受信先機器へ送信する暗号化鍵保持手段とを備えることを特徴とする第1の本発明のバスブリッジである。

【0026】また、第5の本発明（請求項9に記載の本発明に対応）は、前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、前記送信元機器および前記受信先機器とそれぞれ前記ストリームに対応する認証を行う認証手段と、前記データを前記暗号化鍵によって解読する暗号解読手段と、前記解読されたデータをブリッジ用鍵によって再暗号化する再暗号化手段と、前記送信元機器から、前記ストリームに対応する前記暗号化鍵、および、前記暗号化鍵によって暗号化された前記ストリームに対応する前記データを受信する受信手段と、前記ブリッジ用鍵と前記再暗号化されたデータとを前記受信先機器へ送信する送信手段とを備えることを特徴とする第1の本発明のバスブリッジである。

【0027】また、第6の本発明（請求項15に記載の本発明に対応）は、本発明のバスブリッジの各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納することを特徴とする記録媒体である。

【0028】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【0029】（第1の実施の形態）まず、本発明の第1の実施の形態を図面を参照して説明する。

【0030】図1は、本発明の第1の実施の形態におけるバスブリッジの構成を示す構成図である。本実施の形態におけるバスブリッジは、図6で示したバスブリッジ100と同様に、2つのIEEE1394バスが接続されたバスブリッジである。

12

【0031】図1に示すように、本実施の形態におけるバスブリッジ10は、バス1と直接データの転送を行うD-I/F（デジタルインターフェイス）11と、バス2と直接データの伝達を行うD-I/F12と、各バスから送信されてきたパケットに対してクロック調整処理等の従来のバスブリッジと同様の処理を行う主処理手段13と、AVプロトコルに準拠したアイソクロノスパケットのソースIDを付け替えるソースID付替手段14（本発明の「ID付替手段」に対応）とで構成されている。なお、バス1、バス2には、図6と同様に、それぞれ複数の機器101、102、103、複数の機器201、202、203、・・・が接続されている（図示省略）。また、各機器およびバスブリッジに割り当てられているノードIDは、図6と同じとする。

【0032】次に、本実施の形態におけるバスブリッジの動作を、データ送信元の機器およびデータ受信先の機器の動作とともに説明する。ここで送信元の機器がバス1に接続された機器103であり、受信側の機器がバス2に接続された機器202である場合を例として説明する。

【0033】まず、機器103は、図5で示したフォーマットのアイソクロノスパケットに実データおよび必要な情報を書き込んで、バス1へ出力する。このとき、当該アイソクロノスパケット中のソースID906には、バス1内で機器103を特定するための識別子であるノードID「3」が書き込まれている。

【0034】バスブリッジ10の主処理手段13は、D-I/F11を介して、機器103が出力したアイソクロノスパケットをバス1から受け取り、クロック調整等の処理を行う。このとき、ソースID付替手段14は、当該アイソクロノスパケット中のソースID906に書き込まれている、機器103のノードID「3」を、バス2内でバスブリッジ10を特定するための識別子であるノードID「4」に付け替える。ソースID付替手段14によるソースIDの付け替え、および、主処理手段13が行われると、当該アイソクロノスパケットは、D-I/F12を介して、バス2へ出力される。

【0035】機器202は、バス2へ出力されたアイソクロノスパケットを受信し、ソースID906に書き込まれているノードID「4」により、当該アイソクロノスパケットがバスブリッジ10から出力されたものであることを判別できる。

【0036】また、ソースID付替手段14が上記ソースIDの付け替えを送信元のバスおよび受信先のバスと関連づけて記憶する機能を有しておれば、バス2にバス1から転送されるデータのストリーム数が、EMIの各暗号化モード毎に1つ以下の場合、機器202は、当該アイソクロノスパケットの送信元の機器103への別のデータ等の送信を、バスブリッジ10を介して行うこ



13

とができる。なお、バスブリッジ10がバス2においてバスブリッジ自身を特定するノードIDを複数個有している場合は、当該ノードID毎に前記ストリーム数が、EMIの各暗号化モード毎に1つ以下の場合において、機器202は、当該アイソクロノスパケットの送信元の機器103への別のデータ等の送信を、バスブリッジ10を介して行うことができる。

【0037】以上により、本実施の形態におけるバスブリッジは、AVプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が間接的に送信元の機器を判別できるものであることがわかる。

【0038】(第2の実施の形態)次に、本発明の第2の実施の形態を図面を参照して説明する。

【0039】図2は、本発明の第2の実施の形態におけるバスブリッジの構成を示す構成図である。本実施の形態におけるバスブリッジは、第1の実施の形態におけるバスブリッジと同様に、2つのIEEE1394バスが接続されたバスブリッジである。したがって、本実施の形態において、特に説明のないものについては、第1の実施の形態と同じとし、第1の実施の形態と同一符号を付与している構成部材については、特に説明のない限り、第1の実施の形態と同様の機能を持つものとする。

【0040】図2に示すように、本実施の形態におけるバスブリッジ20が、図1で示した第1の実施の形態におけるバスブリッジ10と異なるのは、本発明の「第2のID付替手段」の機能を有するID付替手段21を備えている点である。なお、D-I/F11、12は、本発明の「認証要求送受信手段」、「暗号化鍵送受信手段」および「データ送受信手段」の機能を有するものである。

【0041】次に、本実施の形態におけるバスブリッジの動作を、データ送信元の機器およびデータ受信先の機器の動作とともに説明する。第1の実施の形態と同様に、送信元の機器がバス1に接続された機器103であり、受信側の機器がバス2に接続された機器202である場合を例として説明する。

【0042】まず、機器103は、データ暗号化鍵Kcによって実データを暗号化し、図5で示したフォーマットのアイソクロノスパケットに暗号化された実データおよび必要な情報を書き込んで、バス1へ出力する。このとき、当該アイソクロノスパケット中のソースID906には、バス1内で機器103を特定するための識別子であるノードID「3」が書き込まれている。なお、データ暗号化鍵Kcは、定期的または不定期的に更新生成されるものとする。

【0043】バスブリッジ20の主処理手段13は、D-I/F11を介して、機器103が出力したアイソク

(8)

特開2000-165376

14

ロノスパケットをバス1から受け取り、クロック調整等の処理を行う。このとき、ソースID付替手段14は、当該アイソクロノスパケット中のソースID906に書き込まれている、機器103のノードID「3」を、バス2内でバスブリッジ20を特定するための識別子であるノードID「4」に付け替える。ソースID付替手段14によるソースIDの付け替え、および、主処理手段13が行われると、当該アイソクロノスパケットは、D-I/F12を介して、バス2へ出力される。

【0044】機器202は、バス2へ出力されたアイソクロノスパケットを受信し、当該アイソクロノスパケット中のシフィールド910に格納されているEMI値を読み取り、これが「10」または「11」である場合には、当該アイソクロノスパケット中の実データが暗号化されているものであると判断して、ソースID906に書き込まれているノードID「4」により、当該アイソクロノスパケットがバスブリッジ20から出力されたもの、すなわち、バス2以外のバスから送信されてきたものであることを判別し、実データの解読のために、当該アイソクロノスパケットの送信元(見掛け上はバスブリッジ20、実際は機器103)に対して、認証要求および認証の手続きに関するエイシンクロノスパケットを送信する(バス2へ出力する)。このとき、当該エイシンクロノスパケット中のディスティネーションIDには、バス2を特定するための識別子であるバスID(例えば、「2」)と、バス2内でバスブリッジ20を特定するための識別子であるノードID「4」とが書き込まれており、当該エイシンクロノスパケット中のソースIDには、バス2を特定するための識別子であるバスID「2」と、バス2内で機器202を特定するための識別子であるノードID「2」とが書き込まれている。

【0045】バスブリッジ20の主処理手段13は、D-I/F12を介して、機器202が出力した認証要求および認証の手続きに関するエイシンクロノスパケットをバス2から受け取り、D-I/F11を介して、バス1へ出力する。この間に、ID付替手段21は、当該エイシンクロノスパケット中のディスティネーションIDを、バス2のバスID「2」とバス2内でのバスブリッジ20のノードID「4」との組合せから、バス1のバスID(例えば、「1」)と機器103のノードID「3」との組合せに付け替え、当該エイシンクロノスパケット中のソースIDを、バス2のバスID「2」と機器202のノードID「2」との組合せから、バス1のバスID「1」とバス1内でのバスブリッジ20のノードID「0」との組合せに付け替える。機器103は、バス1へ出力された認証要求および認証の手続きに関するエイシンクロノスパケットを受信し、認証を行い、当該エイシンクロノスパケット中のソースIDから当該エイシンクロノスパケットの送信元(見掛け上はバスブリッジ20、実際は機器202)を判別し、鍵交換用鍵K

15

xによってデータ暗号化鍵Kcを暗号化し、暗号化されたデータ暗号化鍵Kcおよび鍵交換用鍵Kxをそれぞれ異なる暗号化鍵および認証の手続きに関するエイシンクロナスパケット（以下それぞれ「Kc用エイシンクロナスパケット」、「Kx用エイシンクロナスパケット」と記す）に書き込んで、バス1へ出力する。このとき、当該Kc用エイシンクロナスパケットおよびKx用エイシンクロナスパケット中のディスティネーションIDには、バス1のバスID「1」と、バス1内でのバスブリッジ20のノードID「0」とが書き込まれており、当該Kc用エイシンクロナスパケットおよびKx用エイシンクロナスパケット中のソースIDには、バス1のバスID「1」と、機器103のノードID「3」とが書き込まれている。なお、上述したように、データ暗号化鍵Kcは、定期的または不定期的に更新生成されるもので、機器103は、データ暗号化鍵Kcを更新生成する度に、鍵交換用鍵Kxによって新しいデータ暗号化鍵Kcを暗号化し、暗号化された新しいデータ暗号化鍵Kcを別の暗号化鍵および認証の手続きに関するエイシンクロナスパケットに書き込んで、鍵の要求に応じてバス1へ出力する。

【0046】バスブリッジ20の主処理手段13は、D-I/F11を介して、機器103が出力したKc用エイシンクロナスパケットおよびKx用エイシンクロナスパケットをバス1から受け取り、D-I/F12を介して、バス2へ出力する。この間に、ID付替手段21は、当該Kc用エイシンクロナスパケットおよびKx用エイシンクロナスパケット中のディスティネーションIDを、バス1のバスID「1」とバス1内でのバスブリッジ20のノードID「0」との組合せから、バス2のバスID「2」と機器202のノードID「2」との組合せに付け替え、当該Kc用エイシンクロナスパケットおよびKx用エイシンクロナスパケット中のソースIDを、バス1のバスID「1」と機器103のノードID「3」との組合せから、バス2のバスID「2」とバス2内でのバスブリッジ20のノードID「4」との組合せに付け替える。なお、暗号化された新しいデータ暗号化鍵Kcが書き込まれた別の暗号化鍵および認証の手続きに関するエイシンクロナスパケットについても、上記と同様の処理を行う。

【0047】機器202は、バス2へ出力されたKc用エイシンクロナスパケットおよびKx用エイシンクロナスパケットを受信し、当該Kc用エイシンクロナスパケットおよびKx用エイシンクロナスパケット中のソースIDに書き込まれているノードID「4」により、当該Kc用エイシンクロナスパケットおよびKx用エイシンクロナスパケットがバスブリッジ20から出力されたものであることを判別する。そして、得られた鍵交換用鍵Kxによってデータ暗号化鍵Kcを解読し、解読された

(9)

特開2000-165376

16

データ暗号化鍵Kcによって実データを解読する。一度データ暗号化鍵Kcを入手すると、それ以降に送信されてくるアイソクロノスパケットの実データの解読については、新しいデータ暗号化鍵Kcが別の暗号化鍵および認証の手続きに関するエイシンクロナスパケットによって送信されてくるまで、同一のデータ暗号化鍵Kcによって行う。

【0048】以上により、本実施の形態におけるバスブリッジは、AVプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が間接的に送信元の機器を判別できるものであることがわかる。

【0049】また、本実施の形態におけるバスブリッジは、前記アイソクロノスパケットの受信先バス内でバスブリッジ自身を特定するノードID1つに対して、前記受信先バスに前記受信先バス以外の前記バスから転送されるストリーム数が、EMIの各暗号化モード毎に1つ以下の場合は、実データが暗号化されて送信される場合、前記アイソクロノスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われるものであることがわかる。言い換えれば、バスブリッジが前記ストリーム数を上記条件に制限する機能を有しておれば、常に、前記アイソクロノスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われるものであることがわかる。

【0050】なお、本実施の形態においては、本発明の暗号化鍵が、定期的または不定期的に更新生成されるデータ暗号化鍵と、前記データ暗号化鍵の暗号化に用いる鍵交換用鍵とで構成されるとして説明したが、データ暗号化鍵のみで構成される場合は、データ暗号化鍵は暗号化されずに送信され、鍵交換鍵の送信は行われない。

【0051】また、本実施の形態におけるバスブリッジ20のID付替手段21の代わりに、送信元バスおよび送信元機器を特定できる送信元識別子を、アイソクロノスパケットの所定の位置に書き込む識別子書込手段を備えるバスブリッジとすると、受信先機器が、前記アイソクロノスパケットから前記送信元識別子を読み取り、認証要求および認証の手続きに関するエイシンクロナスパケットの所定の位置に、受信先バスおよび前記受信先機器自身を特定できる受信先識別子および前記送信元識別子を書き込んで送信し、D-I/F11、12が、前記認証要求および認証の手続きに関するエイシンクロナスパケットを受信して、前記送信元識別子を読み取り、これに基づいて、前記認証要求および認証の手続きに関するエイシンクロナスパケットを前記送信元機器へ送信し、前記送信元機器が、前記認証要求および認証の手続きに関するエイシンクロナスパケットを受信して、前記送信元識別子を読み取り、暗号化鍵および認証の手続き

17

に関するエイシクロノスパケットの所定の位置に、前記送信元識別子および前記受信先識別子を書き込んで送信し、D-I/F11、12が、前記暗号化鍵および認証の手續きに関するエイシクロノスパケットを受信して、前記受信先識別子を読み取り、これに基づいて、前記暗号化鍵および認証の手續きに関するエイシクロノスパケットを前記受信先機器へ送信することによって、AVプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が直接送信元の機器を判別でき、その上、ストリーム数に関わらず、常に、アイソクロノスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われる。アイソクロノスパケットの所定の位置については、例えば、図5のフォーマット中で各転送に直接関係のない位置を選定して仮想的に送信元識別子を書き込むことになるが、エイシクロノスパケットの所定の位置については、アイソクロノスパケットと同様に選定してもよいし、エイシクロノスパケットのソースIDおよびディステーションIDの位置としてもよい。

【0052】(第3の実施の形態)次に、本発明の第3の実施の形態を図面を参照して説明する。

【0053】図3は、本発明の第3の実施の形態におけるバスブリッジの構成を示す構成図である。本実施の形態におけるバスブリッジは、第1の実施の形態におけるバスブリッジと同様に、2つのIEEE1394バスが接続されたバスブリッジである。したがって、本実施の形態において、特に説明のないものについては、第1の実施の形態と同じとし、第1の実施の形態と同一符号を付与している構成部材については、特に説明のない限り、第1の実施の形態と同様の機能を持つものとする。

【0054】図3に示すように、本実施の形態におけるバスブリッジ30が、図1で示した第1の実施の形態におけるバスブリッジ10と異なるのは、本発明の「認識手段」の機能を有する認識手段31と、本発明の「暗号化鍵保持手段」の機能を有する暗号化鍵保持手段32とを備えている点である。なお、認証手段31は、データの転送要求をしてきた装置(例えば、機器202)との間で、バスブリッジ30およびその装置が正規の装置であるかどうかを互いに確かめ合うため、所定の秘密関数を利用して認証作業を行い、その結果として、認証相手に対応したサブキーを生成する手段である。

【0055】次に、本実施の形態におけるバスブリッジの動作を、データ送信元の機器およびデータ受信先の機器の動作とともに説明する。第1の実施の形態と同様に、送信元の機器がバス1に接続された機器103であり、受信側の機器がバス2に接続された機器202である場合を例として説明する。

【0056】まず、機器103は、データ暗号化鍵Kc

(10)

特開2000-165376

18

によって実データを暗号化し、図5で示したフォーマットのアイソクロノスパケットに暗号化された実データおよび必要な情報を書き込んで、バス1へ出力する。このとき、当該アイソクロノスパケット中のソースID906には、バス1内で機器103を特定するための識別子であるノードID「3」が書き込まれている。なお、データ暗号化鍵Kcは、定期的または不定期的に更新生成されるものとする。

【0057】バスブリッジ30の主処理手段13は、D-I/F11を介して、機器103が出力したアイソクロノスパケットをバス1から受け取り、クロック調整等の処理を行う。このとき、ソースID付替手段14は、当該アイソクロノスパケット中のソースID906に書き込まれている、機器103のノードID「3」を、バス2内でバスブリッジ30を特定するための識別子であるノードID「4」に付け替える。ソースID付替手段14によるソースIDの付け替え、および、主処理手段13が行われると、当該アイソクロノスパケットは、D-I/F12を介して、バス2へ出力される。この間に、認証手段31は、当該アイソクロノスパケット中のシフィールド910に格納されているEMI値を読み取り、これが「10」または「11」である場合には、当該アイソクロノスパケット中の実データが暗号化されているものであると判断して、当該アイソクロノスパケットの送信元である機器103に対して、認証要求および認証の手續きに関するエイシクロノスパケットをD-I/F11、バス1を介して送信する。このとき、当該エイシクロノスパケット中のディステーションIDには、バス1のバスID「1」と、機器103のノードID「3」とが書き込まれており、当該エイシクロノスパケット中のソースIDには、バス1のバスID「1」と、バス1内でのバスブリッジ30のノードID「0」とが書き込まれている。

【0058】機器103は、認証手段31からバス1へ出力された認証要求および認証の手續きに関するエイシクロノスパケットを受信し、認証を行い、当該エイシクロノスパケット中のソースIDから当該エイシクロノスパケットの送信元(バスブリッジ30)を判別し、鍵交換用鍵Kxによってデータ暗号化鍵Kcを暗号化し、暗号化されたデータ暗号化鍵Kcおよび鍵交換用鍵Kxを、それぞれKc用エイシクロノスパケット、Kx用エイシクロノスパケットに書き込んで、鍵の要求に応じてバス1へ出力する。このとき、当該Kc用エイシクロノスパケットおよびKx用エイシクロノスパケット中のディステーションIDには、バス1のバスID「1」と、バス1内でのバスブリッジ30のノードID「0」とが書き込まれており、当該エイシクロノスパケット中のソースIDには、バス1のバスID「1」と、機器103のノードID「3」とが書き込まれている。なお、上述したように、データ暗号化鍵Kc

19

は、定期的または不定期的に更新生成されるものなので、機器103は、データ暗号化鍵Kcnを更新生成する度に、鍵交換用鍵Kxによって新しいデータ暗号化鍵Kcnを暗号化し、暗号化された新しいデータ暗号化鍵Kcnを別の暗号化鍵および認証の手續きに関するエイシンクロナスパケットに書き込んで、鍵の要求に応じてバス1へ出力する。

【0059】一方、機器202は、バス2へ出力されたアイソクロナスパケットを受信し、当該アイソクロナスパケット中のSyフィールド910に格納されているEMI値を読み取り、これが「10」または「11」である場合には、当該アイソクロナスパケット中の実データが暗号化されているものと判断して、ソースID906に書き込まれているノードID「4」により、当該アイソクロナスパケットがバスブリッジ30から出力されたものであることを判別し、実データの解説のために、当該アイソクロナスパケットの送信元（バスブリッジ30）に対して、認証要求および認証の手續きに関するエイシンクロナスパケットを送信する（バス2へ出力する）。このとき、当該エイシンクロナスパケット中のディスティネーションIDには、バス2のバスID「2」と、バス2内でのバスブリッジ30のノードID「4」とが書き込まれており、当該エイシンクロナスパケット中のソースIDには、バス2のバスID「2」と、機器202のノードID「2」とが書き込まれている。

【0060】バスブリッジ30の認証手段31は、D-I/F11を介して、機器103が出力したKc用エイシンクロナスパケットおよびKx用エイシンクロナスパケットをバス1から受け取り、認証を行う。認証が完了すると、暗号化鍵保持手段32は、これらのエイシンクロナスパケットから、暗号化されたデータ暗号化鍵Kcおよび鍵交換用鍵Kxを取り出して保持する。そして、D-I/F12を介して、機器202が出力した認証要求および認証の手續きに関するエイシンクロナスパケットをバス2から受信すると、認証手段31は、認証を行う。認証が完了すると、D-I/F12は、鍵の要求に応じて暗号化鍵保持手段32が保持していた暗号化されたデータ暗号化鍵Kcおよび鍵交換用鍵Kxを、それぞれ異なる暗号化鍵および認証の手續きに関するエイシンクロナスパケット（以下、「新たなKc用エイシンクロナスパケット」および「新たなKx用エイシンクロナスパケット」と記す）に書き込んで、主処理手段13によるクロック調整等の処理を行った後、バス2へ出力する。このとき、当該Kc用エイシンクロナスパケットおよびKx用エイシンクロナスパケット中のディスティネーションIDには、バス2のバスID「2」と、機器202のノードID「2」とが書き込まれており、当該エイシンクロナスパケット中のソースIDには、バス2のバスID「2」と、バス2内でのバスブリッジ30のノ

(11)

特開2000-165376

20

ードID「4」とが書き込まれている。なお、暗号化された新しいデータ暗号化鍵Kcnについても、上記の暗号化されたデータ暗号化鍵Kcと同様の処理を行う。

【0061】機器202は、バス2へ出力されたKc用エイシンクロナスパケットおよびKx用エイシンクロナスパケットを受信し、当該Kc用エイシンクロナスパケットおよびKx用エイシンクロナスパケット中のソースIDに書き込まれているノードID「4」により、当該Kc用エイシンクロナスパケットおよびKx用エイシンクロナスパケットがバスブリッジ30から出力されたものであることを判別する。そして、得られた鍵交換用鍵Kxによってデータ暗号化鍵Kcを解説し、解説されたデータ暗号化鍵Kcによって実データを解説する。一度データ暗号化鍵Kcを入手すると、それ以降に送信されてくるアイソクロナスパケットの実データの解説については、新しいデータ暗号化鍵Kcnが別の暗号化鍵および認証の手續きに関するエイシンクロナスパケットによって送信されてくるまで、同一のデータ暗号化鍵Kcによって行う。

【0062】以上により、本実施の形態におけるバスブリッジは、AVプロトコルに準拠したアイソクロナスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が間接的に送信元の機器を判別できるものであることがわかる。

【0063】また、本実施の形態におけるバスブリッジは、前記アイソクロナスパケットの受信先バス内でバスブリッジ自身を特定するノードID1つに対して、前記受信先バスに前記受信先バス以外の前記バスから転送されるストリーム数が、EMIの各暗号化モード毎に1つ以下の場合は、実データが暗号化されて送信される場合、前記アイソクロナスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われるものであることがわかる。言い換えれば、バスブリッジが前記ストリーム数を上記条件に制限する機能を有しておれば、常に、前記アイソクロナスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われるものであることがわかる。

【0064】なお、本実施の形態においては、本発明の暗号化鍵が、定期的または不定期的に更新生成されるデータ暗号化鍵と、前記データ暗号化鍵の暗号化に用いる鍵交換用鍵とで構成されるとして説明したが、データ暗号化鍵のみで構成される場合は、データ暗号化鍵は暗号化されずに送信され、鍵交換鍵の送信は行われない。

【0065】（第4の実施の形態）次に、本発明の第4の実施の形態を図面を参照して説明する。

【0066】図4は、本発明の第4の実施の形態におけるバスブリッジの構成を示す構成図である。本実施の形態におけるバスブリッジは、第1の実施の形態における

(12)

特開2000-165376

21

バスブリッジと同様に、2つのIEEE1394バスが接続されたバスブリッジである。したがって、本実施の形態において、特に説明のないものについては、第1の実施の形態と同じとし、第1の実施の形態と同一符号を付与している構成部材については、特に説明のない限り、第1の実施の形態と同様の機能を持つものとする。

【0067】図4に示すように、本実施の形態におけるバスブリッジ40が、図1で示した第1の実施の形態におけるバスブリッジ10と異なるのは、本発明の「認識手段」の機能を有する認識手段31（第3の実施の形態で説明した認識手段31と同じもの）と、本発明の「暗号解読手段」の機能を有する暗号解読手段41と、本発明の「再暗号化手段」の機能を有する再暗号化手段42とを備えている点である。なお、D-I/F11、12は、本発明の「受信手段」および「送信手段」の機能を有するものである。

【0068】次に、本実施の形態におけるバスブリッジの動作を、データ送信元の機器およびデータ受信先の機器の動作とともに説明する。第1の実施の形態と同様に、送信元の機器がバス1に接続された機器103であり、受信側の機器がバス2に接続された機器202である場合を例として説明する。

【0069】まず、機器103は、データ暗号化鍵Kcによって実データを暗号化し、図5で示したフォーマットのアイソクロノスケットに暗号化された実データおよび必要な情報を書き込んで、バス1へ出力する。このとき、当該アイソクロノスケット中のソースID906には、バス1内で機器103を特定するための識別子であるノードID「3」が書き込まれている。なお、データ暗号化鍵Kcは、定期的または不定期的に更新生成されるものとする。

【0070】バスブリッジ40の認証手段31は、当該アイソクロノスケット中のSyフィールド910に格納されているEMI値を読み取り、これが「10」または「11」である場合には、当該アイソクロノスケット中の実データが暗号化されているものであると判断して、当該アイソクロノスケットの送信元である機器103に対して、認証要求および認証の手続きに関するエイシンクロノスケットをD-I/F11、バス1を介して送信する。このとき、当該エイシンクロノスケット中のディスティネーションIDには、バス1のバスID「1」と、機器103のノードID「3」とが書き込まれており、当該エイシンクロノスケット中のソースIDには、バス1のバスID「1」と、バス1内のバスブリッジ40のノードID「0」とが書き込まれている。

【0071】機器103は、認証手段31からバス1へ出力された認証要求および認証の手続きに関するエイシンクロノスケットを受信し、認証を行い、当該エイシンクロノスケット中のソースIDから当該エイシンク

22

ロナスケットの送信元（バスブリッジ30）を判別し、鍵交換用鍵Kxによってデータ暗号化鍵Kcを暗号化し、暗号化されたデータ暗号化鍵Kcおよび鍵交換用鍵Kxを、それぞれKc用エイシンクロノスケット、Kx用エイシンクロノスケットに書き込んで、バス1へ出力する。このとき、当該Kc用エイシンクロノスケットおよびKx用エイシンクロノスケット中のディスティネーションIDには、バス1のバスID「1」と、バス1内のバスブリッジ40のノードID「0」とが書き込まれており、当該エイシンクロノスケット中のソースIDには、バス1のバスID「1」と、機器103のノードID「3」とが書き込まれている。なお、上述したように、データ暗号化鍵Kcは、定期的または不定期的に更新生成されるものなので、機器103は、データ暗号化鍵Kc nを更新生成する度に、鍵交換用鍵Kxによって新しいデータ暗号化鍵Kc nを暗号化し、暗号化された新しいデータ暗号化鍵Kc nを別の暗号化鍵および認証の手続きに関するエイシンクロノスケットに書き込んで、鍵の要求に応じてバス1へ出力する。

【0072】バスブリッジ40の認証手段31は、D-I/F11を介して、機器103が出力したKc用エイシンクロノスケットおよびKx用エイシンクロノスケットをバス1から受け取り、認証を行う。認証が完了すると、暗号解読手段41は、これらのエイシンクロノスケットから、暗号化されたデータ暗号化鍵Kcおよび鍵交換用鍵Kxを取り出して、鍵交換用鍵Kxによってデータ暗号化鍵Kcを解読し、解読されたデータ暗号化鍵Kcによって、既に受信されたアイソクロノスケットから得られる暗号化された実データを解読する。再暗号化手段42は、解読された実データを、自らが定期的または不定期的に更新生成するブリッジ用暗号化鍵Kbcによって再暗号化し、このブリッジ用暗号化鍵Kbcをブリッジ用鍵交換用鍵Kbxによって暗号化する。D-I/F12は、再暗号化された実データをバス2へ送信するためのアイソクロノスケットを図5で示したフォーマットに従って生成し、主処理手段13によるクロック調整等の処理を行った後、バス2へ出力する。このとき、ソースID付替手段14は、当該アイソクロノスケット中のソースID906に、バス2内でバスブリッジ40を特定するための識別子であるノードID「4」を書き込む。なお、暗号解読手段41は、一度データ暗号化鍵Kcを入手すると、それ以降に送信されてくるアイソクロノスケットの実データの解読については、新しいデータ暗号化鍵Kc nが別の暗号化鍵および認証の手続きに関するエイシンクロノスケットによって送信されてくるまで、同一のデータ暗号化鍵Kcによって行う。それに対応して、再暗号化手段42は、同一のブリッジ用暗号化鍵Kbcによって再暗号化を行い、新しいデータ暗号化鍵Kc nが送信されてくると、新し

23

いブリッジ用暗号化鍵Kbcnに切り替えて、これによって再暗号化を行い、この新しいブリッジ用暗号化鍵Kbcnをブリッジ用鍵交換用鍵Kbxによって暗号化する。

【0073】機器202は、バス2へ出力されたアイソクロノスパケットを受信し、当該アイソクロノスパケット中のSyフィールド910に格納されているEMI値を読み取り、これが「10」または「11」である場合には、当該アイソクロノスパケット中の実データが暗号化されているものであると判断して、ソースID906に書き込まれているノードID「4」により、当該アイソクロノスパケットがバスブリッジ40から出力されたものであることを判別し、実データの解説のために、当該アイソクロノスパケットの送信元（バスブリッジ40）に対して、認証要求および認証の手続きに関するエイシンクロノスパケットを送信する（バス2へ出力する）。このとき、当該エイシンクロノスパケット中のディステーションIDには、バス2のバスID「2」と、バス2内でのバスブリッジ40のノードID「4」とが書き込まれており、当該エイシンクロノスパケット中のソースIDには、バス2のバスID「2」と、機器202のノードID「2」とが書き込まれている。

【0074】バスブリッジ40の認証手段31は、D-1/F12を介して、機器202が出力した認証要求および認証の手続きに関するエイシンクロノスパケットをバス2から受信すると、認証を行う。認証が完了すると、D-1/F12は、暗号化されたブリッジ用暗号化鍵Kbcおよびブリッジ用鍵交換用鍵Kbxを、それぞれ異なる暗号化鍵および認証の手続きに関するエイシンクロノスパケット（以下、「新たなKbc用エイシンクロノスパケット」および「新たなKbx用エイシンクロノスパケット」と記す）に書き込んで、鍵の要求に応じてバス2へ出力する。このとき、当該Kbc用エイシンクロノスパケットおよびKbx用エイシンクロノスパケット中のディステーションIDには、バス2のバスID「2」と、機器202のノードID「2」とが書き込まれており、当該エイシンクロノスパケット中のソースIDには、バス2のバスID「2」と、バス2内でのバスブリッジ40のノードID「4」とが書き込まれている。なお、ブリッジ用暗号化鍵Kbcが新しいブリッジ用暗号化鍵Kbcnに切り替えられた場合において、新しいブリッジ用暗号化鍵Kbcnの転送上の取扱いは、ブリッジ用暗号化鍵Kbcと同様である。

【0075】機器202は、バス2へ出力されたKbc用エイシンクロノスパケットおよびKbx用エイシンクロノスパケットを受信し、当該Kbc用エイシンクロノスパケットおよびKbx用エイシンクロノスパケット中のソースIDに書き込まれているノードID「4」により、当該Kc用エイシンクロノスパケットおよびKx用エイシンクロノスパケットがバスブリッジ40から出力

(13)

特開2000-165376

24

されたものであることを判別する。そして、得られたブリッジ用鍵交換用鍵Kbxによってブリッジ用暗号化鍵Kbcを解説し、解説されたブリッジ用暗号化鍵Kbcによって実データを解説する。一度ブリッジ用暗号化鍵Kbcを入手すると、それ以降に送信されてくるアイソクロノスパケットの実データの解説については、新しいブリッジ用暗号化鍵Kbcnが別の暗号化鍵および認証の手続きに関するエイシンクロノスパケットによって送信されてくるまで、同一のブリッジ用暗号化鍵Kbcによって行う。

【0076】以上により、本実施の形態におけるバスブリッジは、AVプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が間接的に送信元の機器を判別できるものであることがわかる。

【0077】また、本実施の形態におけるバスブリッジは、前記アイソクロノスパケットの受信先バスに前記受信先バス以外の前記バスから転送されるストリーム数に関わらず、実データが暗号化されて送信される場合、前記アイソクロノスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われるものであることがわかる。

【0078】なお、本実施の形態においては、本発明の暗号化鍵が、定期的または不定期的に更新生成されるデータ暗号化鍵と、前記データ暗号化鍵の暗号化に用いる鍵交換用鍵とで構成され、本発明のブリッジ用鍵が、定期的または不定期的に更新生成されるブリッジ用暗号化鍵と、前記ブリッジ用暗号化鍵の暗号化に用いるブリッジ用鍵交換用鍵とで構成されるとして説明したが、本発明の暗号化鍵が、データ暗号化鍵のみで構成される場合は、本発明のブリッジ用鍵はブリッジ用暗号化鍵のみで構成され、データ暗号化鍵およびブリッジ用暗号化鍵は暗号化されずに送信され、鍵交換鍵およびブリッジ用鍵交換用鍵の送信は行われない。

【0079】また、本実施の形態においては、本発明のブリッジ用暗号化鍵およびブリッジ用鍵交換用鍵は、バスブリッジが固有に生成したものであるとして説明したが、これに限らず、1つの送信元機器から送信されてくるストリームに対応するデータ暗号化鍵Kcおよび/または鍵交換用鍵Kxを、それぞれブリッジ用暗号化鍵Kbcおよび/またはブリッジ用鍵交換用鍵Kbxとして、当該ストリームに対応する解説・再暗号化の全部または一部を省略することができる。具体的には、以下の3ケースが想定される。

【0080】1番目のケースは、ブリッジ用暗号化鍵Kbcおよびブリッジ用鍵交換用鍵Kbxが、1つのストリームに対応するデータ暗号化鍵Kcおよび鍵交換用鍵Kxとそれぞれ同じ場合である。この場合、このストリ



25

ームに対しては、ブリッジ用暗号化鍵Kbcと同じデータ暗号化鍵Kcにより暗号化された実データと、ブリッジ用鍵交換用鍵Kbxと同じ鍵交換用鍵Kxにより暗号化されたデータ暗号化鍵Kbc（すなわち、Kc）は、暗号解読手段41による解読および再暗号化手段42による再暗号化を行われず、機器202（受信先機器）へ送信される。他のストリームに対しては、本実施の形態において説明したのと同様に解読が行われ、ブリッジ用暗号化鍵Kbc（すなわち、前記1つのストリームに対応するデータ暗号化鍵Kc）およびブリッジ用鍵交換用鍵Kbx（すなわち、前記1つのストリームに対応する鍵交換用鍵Kx）によって、本実施の形態において説明したのと同様に実データ等の再暗号化が行われる。

【0081】2番目のケースは、ブリッジ用暗号化鍵Kbcのみが、1つのストリームに対応するデータ暗号化鍵Kcと同じ場合である。この場合、このストリームに対しては、D-I/F11（本発明の受信手段）は、機器103（送信元機器）から、データ暗号化鍵Kcによって暗号化された実データ、鍵交換用鍵Kxによって暗号化されたデータ暗号化鍵Kcおよび鍵交換用鍵Kxを受信し、暗号解読手段41は、データ暗号化鍵Kcを鍵交換用鍵Kxによって解読し、再暗号化手段42は、データ暗号化鍵Kcをブリッジ用暗号化鍵Kbcとし、これをバスブリッジ40で生成されたブリッジ用鍵交換用鍵Kbxによって再暗号化する。このとき、暗号解読手段41は実データの暗号化を行わず、したがって、再暗号化手段42も実データの再暗号化は行わない。そして、D-I/F12（本発明の送信手段）は、ブリッジ用鍵交換用鍵Kbc、ブリッジ用鍵交換用鍵Kbxによって再暗号化されたブリッジ用暗号化鍵Kbcと、暗号解読手段41による解読および再暗号化手段42による再暗号化が行われなかった実データとを機器202（受信先機器）へ送信する。他のストリームに対しては、本実施の形態において説明したのと同様に解読が行われ、ブリッジ用暗号化鍵Kbc（すなわち、前記1つのストリームに対応するデータ暗号化鍵Kc）およびブリッジ用鍵交換用鍵Kbxによって、本実施の形態において説明したのと同様に実データ等の再暗号化が行われる。

【0082】3番目のケースは、ブリッジ用鍵交換用鍵Kbxのみが、1つのストリームに対応する鍵交換用鍵Kxと同じ場合である。この場合、このストリームに対しては、D-I/F11（本発明の受信手段）は、機器103（送信元機器）から、データ暗号化鍵Kcによって暗号化された実データ、鍵交換用鍵Kxによって暗号化されたデータ暗号化鍵Kcおよび鍵交換用鍵Kxを受信し、暗号解読手段41は、データ暗号化鍵Kcを鍵交換用鍵Kxによって解読し、実データを解読されたデータ暗号化鍵Kcによって解読する。再暗号化手段42は、解読されたデータを、バスブリッジ40で生成されたブリッジ用暗号化鍵Kbcによって再暗号化し、鍵交

(14)

特開2000-165376

26

換用鍵Kxをブリッジ用鍵交換用鍵Kbxとし、これによってブリッジ用暗号化鍵Kxを再暗号化する。そして、D-I/F12（本発明の送信手段）は、ブリッジ用鍵交換用鍵Kbc、ブリッジ用鍵交換用鍵Kbxによって再暗号化されたブリッジ用暗号化鍵Kbcと、暗号解読手段41による解読および再暗号化手段42による再暗号化が行われなかった実データとを機器202（受信先機器）へ送信する。他のストリームに対しては、本実施の形態において説明したのと同様に解読が行われ、ブリッジ用暗号化鍵Kbcおよびブリッジ用鍵交換用鍵Kbx（すなわち、前記1つのストリームに対応する鍵交換用鍵Kx）によって、本実施の形態において説明したのと同様に実データ等の再暗号化が行われる。

【0083】なお、上述した第1～第4の実施の形態におけるバスブリッジは、2つのIEEE1394バスが接続されたバスブリッジであるとして説明したが、これに限るものではなく、AVプロトコルに準拠したアイソクロノスケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行うバスブリッジであればよい。接続するバスブリッジの数も2つに限らず、複数であればよい。3つ以上のバスが接続される場合であっても、1つのバスに他のバスからデータ転送が行われる場合の取扱い、第1～第4の実施の形態において説明したのと同様である。

【0084】また、上述した第1～第4の実施の形態においては、本発明のバスブリッジを中心に説明したが、本発明の記録媒体としては、以上説明した各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納する記録媒体が挙げられる。

【0085】

【発明の効果】以上説明したところから明らかなように、請求項1の本発明は、AVプロトコルに準拠したアイソクロノスケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が直接または間接的に送信元の機器を判別できるバスブリッジを提供することができる。

【0086】また、請求項2～14の本発明は、請求項1の本発明の効果に加え、実データが暗号化されて送信される場合、前記送信元の機器と前記受信先の機器との間での認証・鍵交換が確実に行われるバスブリッジを提供することができる。

【0087】また、請求項15の本発明は、本発明のバスブリッジの各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納する記録媒体を提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態におけるバスブリッジの構成を示す構成図である。



(15)

特開2000-165376

27

28

【図2】本発明の第2の実施の形態におけるバスブリッジの構成を示す構成図である。

【図3】本発明の第3の実施の形態におけるバスブリッジの構成を示す構成図である。

【図4】本発明の第4の実施の形態におけるバスブリッジの構成を示す構成図である。

【図5】AVプロトコルに準拠したアイソクロノスパケットのフォーマットを示す図である。

【図6】バスブリッジによってデータ転送の仲介が行われる2つのIEEE1394バスを示す概略構成図である。

【符号の説明】

1、2 バス

10、20、30、40、100 バスブリッジ

11、12 D-I/F

13 主処理手段

14 ソースID付替手段

21 ID付替手段

31 認証手段

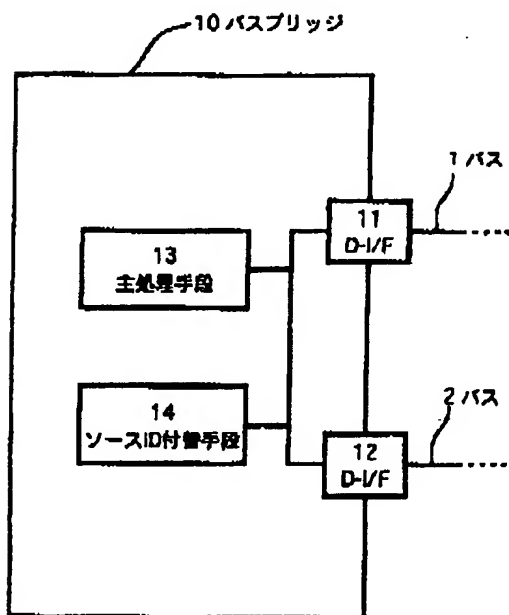
32 暗号化鍵保持手段

41 暗号解読手段

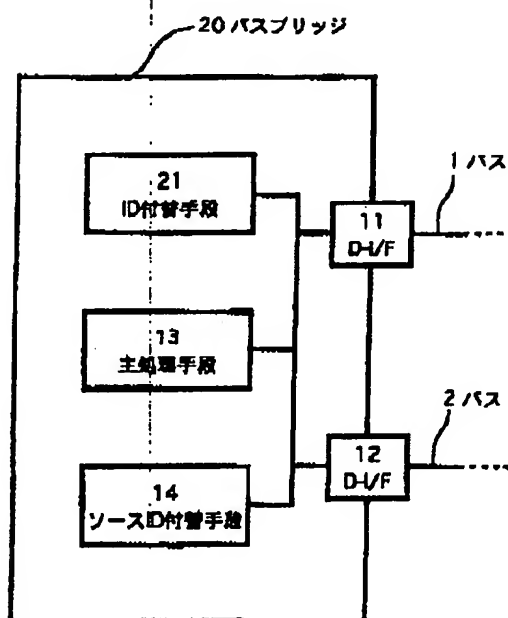
42 再暗号化手段

101、102、103、201、202、203 機器

【図1】



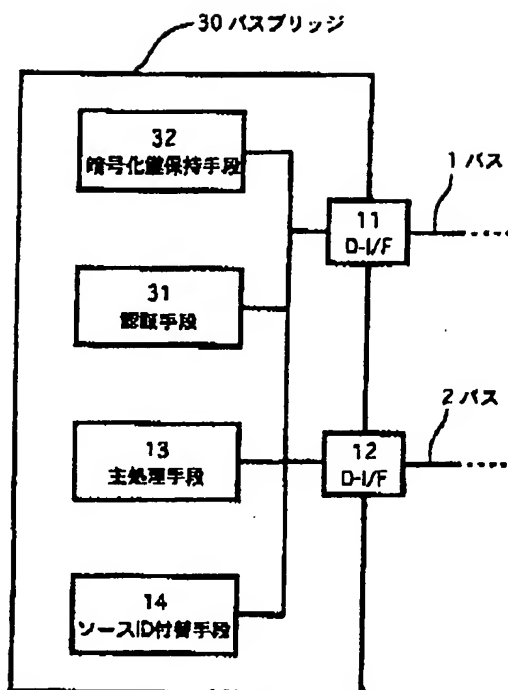
【図2】



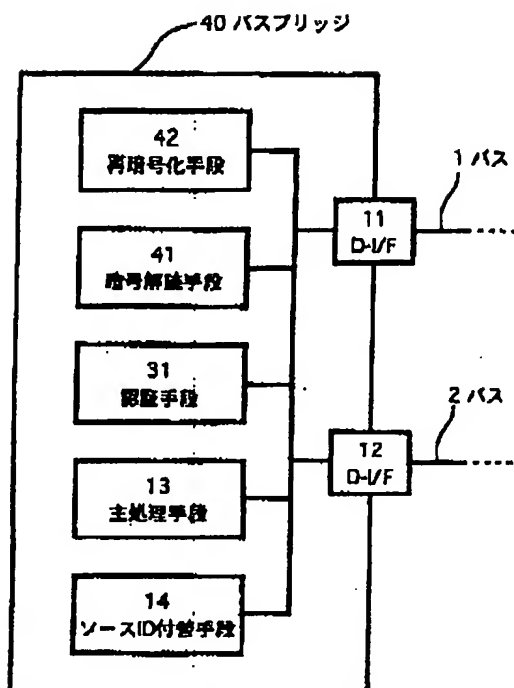
(16)

特開2000-165376

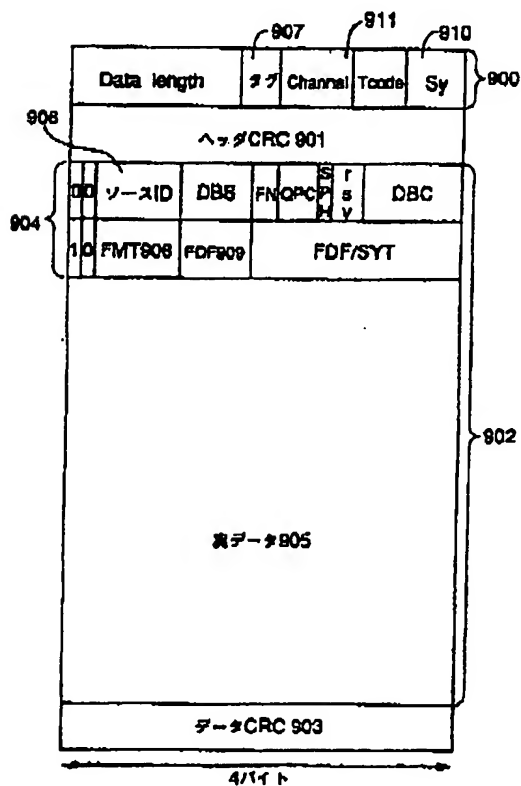
【図3】



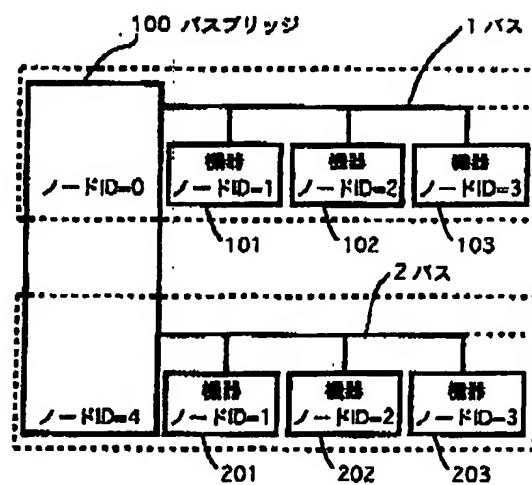
【図4】



【図5】



【図6】



(17)

特開2000-165376

フロントページの続き

(72)発明者 西村 拓也

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72)発明者 武知 秀明

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72)発明者 久野 良樹

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72)発明者 浜本 康男

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

Fターム(参考) 6D044 DE49 GK17 HL11

5J104 AA07 KA02 KA04 PA07

5K033 AA08 CB01 CB09 CC01 CC04

DA13 DB18

Title of the Prior Art

Japanese Published Patent Application No. H12-165376

Date of Publication: June 16, 2000

Concise Statement of Relevancy

(1) Translation of paragraphs [0002]-[0013].

[0002]

[Background Art] Recently, high-speed serial bus interface (hereinafter described as 「IEEE1394 bus」 that employ IEEE 1394 specification (IEEE: THE INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS, INC) has been paid attention; digital interface which play a large amount of data transfer in high speed and high quality.

[0003] As data transfer in IEEE 1394 specification, there are an isochronous communication which is suited to transfer of synchronous data such as video signal or audio signal as well as an asynchronous communication which is suited to transfer of asynchronous data such as control signals. Both of these communications can co-exist on IEEE1394bus.

[0004] The isochronous communication is a so-called communication of broadcast type, and isochronous packet which is output from a certain apparatus on IEEE1394 bus can be received by all of the apparatus connected on the bus.

[0005] On the other hand, asynchronous communication has both communication, one-to-one communication and broadcast-type communication. An asynchronous packet which is output from a certain apparatus on the bus, includes a destination ID which represents an apparatus which should receive the packet inside the packet-header. When the destination ID represents a certain apparatus, an apparatus which is indicated by the identifier receives aforementioned asynchronous packet. When the destination ID represents broadcast, all apparatus on the same bus receive aforementioned asynchronous packet. Also,

asynchronous packet has, inside of packet-header, a source ID as an identifier which represents a sending apparatus that is sending the packet. The destination ID and the source ID have respectively been assigned 16 bit, and in 10 bit of them, a bus ID which identify a bus to which a device is connected is written in, and in 6 bit of them, a node ID which identify aforementioned device on the bus.

[0006] Additionally, IEC61883 specification (hereinafter described as "AV protocol") is considered in IEC(IEC: International Electrotechnical Commission) as a specification for conducting a connection management of data transfer between devices on IEEE 1394 bus, and a transfer digital audio signal and digital image signal and the like with the use of IEEE 1394 specification. In AV protocol, image audio data is transferred disposed inside the isochronous packet. Additionally, the isochronous packet includes CIP header (CIP: Common Isochronous Packet). The CIP header includes information such as identification data which represents type of image audio data or a source ID as an identifier which represents sending apparatus of sending isochronous packet.

[0007] Figure 5 represents a format of isochronous packet which is in accordance with AV protocol. Isochronous packet consists of isochronous packet-header 900, header CRC 901, isochronous payload 902, and data CRC 903.

[0008] Isochronous packet-header 900 includes tag 907. Tag 907, when the value is 1, indicates that the isochronous packet is one which is in accordance with AV protocol. When the value of tag 907 is 1, in other words, it is one which is in accordance with AV protocol, CIP header 904 is included at the top of the isochronous payload 902.

[0009] Additionally, Channel field 911 in isochronous packet-header 900, is written channel code, and used as a

transfer on the bus.

[0010] Additionally, isochronous packet-header 900 includes Sy field 910. In an isochronous packet of AV protocol compliance, Sy field is used for storing the data protect information (use license information). Specifically, it includes 2 bit information which indicates representative value of use license information (it is called EMI; Encryption Mode Indicator) and data encryption mode and 1 bit information which is called as Odd/Even flag which indicate renewal timing of data encryption key. When the value of EMI which is stored in Sy field 910 indicates 「00」, it indicates data to be sent(actual data 905 described later) is a data that is free to copy. Additionally, when it is 「10」, the data shows that only one time copying is possible, and when it is 「11」, it indicates the data is copy inhibited.

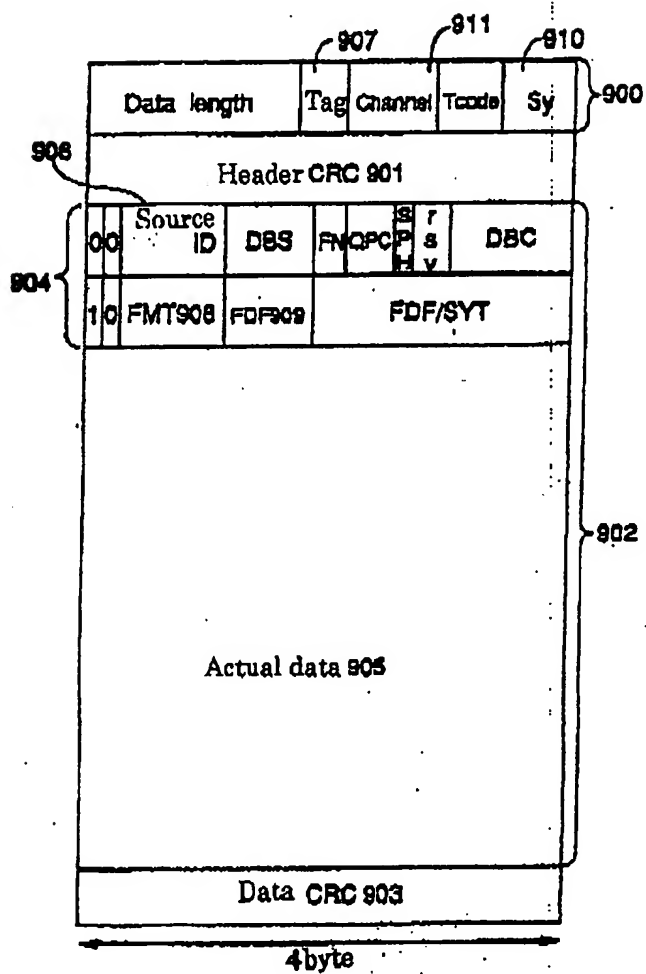
[0011] In the CIP header 904, a source ID 906 which is an identifier of source apparatus which is outputting aforementioned isochronous packet. This source ID 906 has 6 bit in length, and a node ID that identifies the apparatus of aforementioned source in one bus.

[0012] Additionally, the CIP header 904 includes FMT 908 that represents that what kind of data the actual data 905 in isochronous payload 902 or FDF 909.

[0013] Data as objects to be sent such as image and audio are included in actual data 905. This actual data 905 is encrypted data when above-mentioned EMI value is 「10」 or 「11」, while when it is 「00」 which means copy free, it is not encrypted. Additionally, actual use license information is included in the actual data 905, and generally it is called as SCMS, in case of CD, and it is called as such as CGMS in case of DV.

(2) Figure 5 is attached hereto.

[Fig.5]





**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**